Показатели

Определение: *Показателем* остатка a по модулю m является наименьшее такое число t, что

$$a^t \equiv 1 \pmod{m}.$$

Обычно обозначается $ord_m(a)$

Свойства:

$\boxed{1}$ Покажите, что если $(a, m) = 1$, то показатель существует

$\boxed{2}$ Покажите, что если $(a, m) \neq 1$, то показателя не существует.

$\boxed{3}$ Пусть t — показатель a по модулю m.

(a) Докажите, что если $a^k \equiv 1 \pmod{m}$, то $k \,\vdots\, t$.

(b) Докажите, что если $a^{t_1} \equiv a^{t_2} \pmod{m}$, то $t_1 \equiv t_2 \pmod{t}$.

(c) Докажите, что числа $a^0, a^1, a^2, \ldots, a^{t-1}$ попарно различны по модулю m.

$\boxed{4}$ Докажите, что показатели взаимно обратных чисел совпадают.

$\boxed{5}$ Пусть $ord_m(a) = t, ord_m(b) = d$.

(a) Докажите, что если $t \,\vdots\, h$, то $ord_m(a^h) = \dfrac{t}{h}$.

(b) Докажите, что $ord_m(a^h) = \dfrac{t}{(t, h)}$.

(c) Докажите, что если $(t, d) = 1$, то $ord_m(a \cdot b) = t \cdot d$.

Задачи:

$\boxed{1}$ Найдите $ord_{a^n-1}(a)$.

$\boxed{2}$ Докажите, что $\varphi(a^n - 1)$ делится на n для натуральных a и n.

$\boxed{3}$ Рассмотрим все числа вида $10^i - 10^j$ при $0 \leqslant i < j \leqslant 99$. Сколько из них делятся на 1001?

$\boxed{4}$ Дано нечётное простое число p, а также простые числа q и r. Известно, что $q^r + 1 \,\vdots\, p$. Докажите, что либо $p - 1 \,\vdots\, 2r$, либо $q^2 - 1 \,\vdots\, p$.

$\boxed{5}$ Сколько делителей от 1 до 200 имеет число $2^{239} - 1$?

$\boxed{6}$ (a) Докажите, что в разложении на простые сомножители числа $2^q - 1$, где q простое, любое число будет давать остаток 1 по модулю q.

(b) Выведите из этого, что простых чисел бесконечно много.

$\boxed{7}$ Пусть $a > 1, p > 2$ и p простое. Докажите, что простые нечетные делители $a^p - 1$ или делят $a - 1$ или сравнимы с 1 по модулю $2p$.

$\boxed{8}$ Докажите, что любой простой делитель числа $2^{2^k} + 1$ сравним с 1 по модулю 2^{k+1}.

$\boxed{9}$ Даны натуральные числа $a, n > 1$. Докажите, что для каждого нечетного простого делителя p числа $a^{2^n} + 1$ число $p - 1$ делится на 2^{n+1}.

$\boxed{10}$ Дано простое число p. Докажите, что $2^{2^p} - 4$ делится на $2^p - 1$.

$\boxed{11}$ Пусть p и q простые, $q > 5$. Известно, что $2^p + 3^p$ делится на q. Докажите, что $q > 2p$.

$\boxed{12}$ Докажите, что при натуральном $n > 1$ число $2^n - 1$ не делится на n.

$\boxed{13}$ Найдите все пары простых чисел p и q таких, что $(5^p - 2^p)(5^q - 2^q) \vdots pq$.